Patent Claims:

1. A method for the generation of forgery-proof documents or data records, whereby key information is generated and whereby encrypted checking information is formed from the key information and from a transaction indicator, characterized in that
the generation of the random key information and the formation of the encrypted checking information from the key information and from the transaction indicator are carried out in a cryptographically reliable contact station, in that the cryptographically reliable contact station encrypts the key information, and in that the encrypted checking information and the encrypted key information are transmitted by the cryptographically reliable contact station to an intermediate station, in that the intermediate station temporarily stores the encrypted key information and the encrypted checking information and transmits it to a cryptographic module of a document producer later on, at a different point in time from the transfer between the cryptographically reliable contact station and the intermediate station.

2. The method according to Claim 1, characterized in that
the key information is generated in such a way that the key information is formed randomly.

3. The method according to one or more of the preceding claims, characterized in that
the encrypted key information and/or the encrypted checking information is configured in such a way that it cannot be decrypted in the intermediate station.

4. The method according to one or more of the preceding claims, characterized in that
the cryptographic module preferably decrypts the key information with a key contained in the cryptographic module.

5. The method according to one or more of the preceding claims, characterized in that the document producer enters his own data into the cryptographic module.

6. The method according to one or more of the preceding claims, characterized in that the data entered by the document producer is irreversibly linked to the key information by means of the cryptographic module.

7. The method according to Claim 6, characterized in that the data entered by the document producer and the decrypted key information are irreversibly linked in that the key information is used to form a check value for the document.

8. The method according to one or both of Claims 6 or 7, characterized in that the result of the irreversible linking of the data entered by the document producer with the decrypted key information forms a document and/or a data record that is transmitted to a checking station

9. The method according to Claim 8, characterized in that the document transmitted to the checking station contains the document producer's own data, at least partially in plain text.

10. The method according to one or both of Claims 8 or 9, characterized in that the encrypted checking information is entered into the document that is transmitted to the checking station.

11. The method according to one or more of the preceding claims, characterized in that information remaining in the cryptographic module is encrypted in such a way that it can be decrypted in the cryptographic module.

12. The method according to one or more of the preceding claims, characterized in that
the supply of the cryptographic module with the information, also in case of a supply via communication partners that are not reliable in the cryptographic sense, is carried out by a cryptographically reliable station whose information can be relied on by the checking station.

13. The method according to Claim 12, characterized in that, in order for a reliable station to provide reliable information for the cryptographic module, cryptographic encryptions are used that the checking station can reverse.

14. The method according to one or more of Claims ... to 13, characterized in that
the supply of the cryptographic module via communication partners that are cryptographically non-reliable is carried out in such a way that the information is forwarded to the cryptographic module at a different point in time.

15. The method according to one or more of Claims 1 to 14, characterized in that
the supply of the cryptographic module via communication partners that are cryptographically not reliable is carried out in such a way that an exchange of information within a dialog is not necessary.

16. The method according to one or more of Claims 1 to 14, characterized in that
the two types of data are cryptographically linked to each other, but cannot be discovered by means of crypto-analysis.

17. The method according to Claim 19, characterized in that
the cryptographic linking of the two types of data is such that non-linear fractions are added that are known only to the reliable contact station and to the checking station.

18. The method according to one or more of the preceding claims, characterized in that
the generated forgery-proof documents or data records contain monetary value information.

19. The method according to Claim 18, characterized in that
the monetary value information is cryptographically connected to the document or data record in such a way that a check value can be formed by comparing the monetary value information to the document or data record.

20. The method according to one or both of Claims 18 or 19, characterized in that
the monetary value information contains proof of the payment of postage amounts.

21. The method according to Claim 20, characterized in that
the monetary value information that proves the payment of postage amounts is linked to identification data of the document producer.

22. The method according to one or both of Claims 20 or 21, characterized in that
the monetary value information is linked to address data.

23. A value transfer center with an interface for loading monetary values, characterized in that
the value transfer center contains an interface to receive encrypted information of a cryptographically reliable contact station and to temporarily store the received encrypted information.

24. The value transfer center according to Claim 23, characterized in that
the information is encrypted in such a way that it cannot be decrypted in the value transfer center.

25. The value transfer center according to one or more of Claims 23 to 24, characterized in that it contains means for receiving value transfer requests by at least one cryptographic module and for forwarding the received encrypted information at a different point in time.

26. A cryptographic module for generating forgery-proof documents with means to issue encrypted checking information and a check value, characterized in that the cryptographic module contains at least one means for receiving and decrypting key information and at least one means for receiving a document or a data record, and in that the cryptographic module has at least one means to form a check value for the document or for the data record using the key information.